A framework for systems security. (information systems)
Cecere, Carl; Ruppert, William H.
Journal of Electronic Defense , Volume: 15 , Number: 1 , Page: 54(4) , Jan 1992

A Framework for Systems Security

During the development of an action plan for the Defense-Wide Information Systems Security Program[1] (see "Defining a Security Architecture for the Next Century" by John C. Nagengast on p. 51 of this issue), we discovered similarities in security requirements and architectures for a number of major DOD programs. However, no two programs represented their requirements and security architectures in the same way.

The DISSP Architecture and Requirements Working Groups developed a framework that was pioneered by Dennis Grayson of NSA.[2] This framework proved a success for surveying and describing the requirements for five existing systems/programs. This paper will provide the reader with an overview of the framework and a discussion of its implementation for documenting security requirements, and security architectures.

DESCRIPTION

The framework consists of a three-dimensional matrix for mapping security attributes to system elements and protocol layers (Figure 1). The three dimensions are generally orthogonal, and together provide a simple method for illustrating complex information systems.

As can be seen in the figure, the first dimension identifies nine major categories of security attributes. The second dimension identifies system elements. This refers to the features of the information systems concerned with requirements and affords a simplified means for mapping security attributes to system features or elements. The third dimension identifies Open Systems Interconnection (OSI) layers, with an extension of two layers. The OSI model is communications oriented. The additional layers are an expansion to accommodate information processing aspects. OSI layers will not be factored into this paper.

SECURITY ATTRIBUTES

DIMENSION

The starting point in structuring the Security Attributes Dimension of the framework was the description of security services in the ISO 7498 Addendum, Security Architecture. Several categories in the ISO treatment were streamlined and additional attributes were added.

In applying this dimension, it was determined that the nine categories sufficed to define architectures. However, they needed to be subdivided for comparing systems and to foster mutual understanding of definitions. Currently, the NSA is developing a more rigorous set of security attributes for inclusion in the framework.

The following is a brief description/list of the nine attributes, plus the two operational categories, and their respective security requirements subcategories. The subcategories are based on preliminary work completed by an NSA Architecture Working Group as well as on OSI definitions and are by no means the final description of security services or mechanisms. 1) Physical, Procedural and Personal Security. Subcategories: facility clearance level; operational procedures; data classification range; personnel clearances; mode of operation; security administrative roles and responsibilities; applicable regulations, policies, etc.; start up and shut down; recovery; security violation detection; capture/overrun protection. 2) Confidentiality: prevents unauthorized disclosure of information. Subcategories: damage limitation, perishability, sensitivity grading, aggregation, traffic flow security and interference. 3) Accountability: ensures the actions of an entity may be traced uniquely to the entity. Subcategories: identification and audit. 4) Authentication: establishes the validity of a claimed identity. Subcategories: mutual authentication(s) and source authentication. 5) Access Control: prevents unauthorized use of a resource or the use of a resource in an unauthorized manner. Subcategories: identity-based access control, rule-based access control, environment-based access control, content-dependent access control, labeling of data, covert channel management and process confidentiality. 6) Integrity: assures that a system meets an a priori expectation of quality. Subcategories: data integrity, management integrity, process integrity and process sequence integrity. 7) Nonrepudiation: takes one of two forms. Nonrepudiation with proof of origin protects against a sender attempting to falsely deny sending data or its contents; non-repudiation with proof of delivery protects against a recipient attempting to subsequently deny receiving data or its contents. 8) Availability: allows the system to continue to function while degraded or under attack; minimizes the advantage gained by an enemy during adverse conditions. Subcategories: survivability and damage limitation. 9) Assurance: yields confidence in the security features and architectures of a system to accurately mediate and enforce security measures according to security policy. Subcategories: minimum assurance level and system activities. 10) Interoperability: allows protocols and systems to interface. 11) Performance. Subcategories: delay, error rate, probability of delivery and volume.

SYSTEMS ELEMENTS

DIMENSION

The System Elements Dimension allows the system engineer and program manager to consider which of the elements will go into the makeup of a particular system and to map those elements with the security attributes from the Security Attributes Dimension. The System Elements Dimension is portrayed in Figure 2.

This model was chosen because it represents a layered connection of components typically found in information systems. There are many models which may be used. This one enables a simplified discussion of the four elements (networks, end systems, security management and interfaces), applications and requirements.

End Systems

The upper-layer components of Figure 2 are redundant and "mirrored" to address both direct connection to long-haul networks and locally connected devices that may also eventually be connected to long-haul networks.

As illustrated, at the upper layer of the model is the user, which represents people, missions, data and other forms of information, etc. Below that is a local access device, such as a terminal, that allows the user to enter, display, view, etc., the information. Note that if the user has a workstation rather than a terminal, the functionality of the next lower layer is included; if not, then the terminal may be directly

connected or "networked" to a host device.

Hosts and servers are on the same level, as they both provide processing and involve common components such as applications software, operating systems and storage devices. Servers may be of many types, including those for names, data bases, key distribution functions, etc.

The bottom of this layer includes the interfaces necessary for either local or wide area networking.

Network Systems

A network system is one which is implemented with a collection of interconnected network components. The model portrays local networks and wide area networks.

Local networks may include local area networks, private branch exchanges and any other technologies or components, hardware or software, that may be used to implement the network. Wide area networks (WANs) generally use public telecommunications facilities to provide users access to processing facilities associated with the mainframes and to permit highspeed data exchange within the network over a wide geographic area. Components of WANs are similar to those of local networks and end systems. Processors and computers control switching functions and network management data, just as they control user data in end systems and management data in local networks.

Interfaces

Interfaces consist of components (relays) that are necessary to connect local area networks to local area networks or local area networks to long-haul networks, or to interconnect long-haul networks. Routers, bridges, gateways and protocol converters are four common types of relays. Network interface components, to include guards, have become important when considering security in that they are often regarded and implemented as a "band-aid" to connect independent and uncoordinated network development activities.

Security Management

Security management is an integral part of the other elements, but it is sufficiently important to be given special consideration. Security management is categorized in ISO 7498-2 as three separate activities: system security management, security service management and security mechanism management.[3]

OSI DIMENSION

This dimension of the framework consists of the basic seven OSI layers plus a Subject layer and an Operations layer. Subjects include a person, agency, country or computer. Operations consist of functions such as file transfer, data base access, conferencing, directory service or spread sheet.

The OSI dimension is more critical in assessing architectures and architectural alternatives from the standpoint of interoperability, consistency with evolving standards efforts and long-term life cycle costs.

MAPPING SECURITY

REQUIREMENTS TO SYSTEM

ELEMENTS

The rest of this paper addresses the consideration of the elements and security aspects dimensions. Confidentiality will be discussed as a sample statement of requirements and an example solution to illustrate the framework's application. Similar comparisons for all attributes can be done. Such a process must be conducted early in the development phase.

As shown in Table 1, consideration of security requirements starts at the top layer of Figure 2 and continues through each layer of the network model. [Tabular Data Omitted]

End System

* User/Data: If there is a requirement to protect the data from disclosures, consider physical means, encrypted storage and cleared people as typical solutions. * Access: All of the above apply, plus there may be a concern about tampering with the terminal or workstation. If this is a terminal-to-host situation, the connection may need to be protected. Encryption is typical for that requirement. * Processing: Authenticated access to the processes must be reemphasized as a means to protect information from being disclosed. Trusted machines and processes may be necessary. Encrypted storage may be employed, too.

Interfaces

* Net Interface: Information should be presented to the network interface in a manner that ensures it is not disclosed during communications. Encryption is a typical solution. * WAN Interfaces: Red data in gateways may require protected facilities and cleared personnel. Sensitive addresses for Black (encrypted) data may result in the same requirement.

Networks

* Networking: The same considerations apply as for the interface. * Wide Area Network: End-system-to-end-system and end-system-to-interface data (perhaps even addresses) should be protected. End-to-end encryption is typical over the network; link encryption is typical for end-system-to-interface connections. If traffic flow security is a requirement, data flow may be hidden using key generators. * Switches/Trunks: The same considerations must be given to the switches and trunks as given to the interfaces.

Security Management

* Audit and other management data in the network management center (NMC in the table) must be protected. Similarly, consideration must be given to protecting keys and user profile data in the key distribution centers (KDC in the table). Physically secured facilities and encrypted files are typical solutions.

SUMMARY

The above example was presented to demonstrate the value of the framework in mapping security requirements to network components. As stated earlier, the framework is by no means complete. Its publication is intended to foster interest and to obtain comments on how well it serves its intended purpose.

It is hoped this framework will evolve into a security methodology that will aid in identifying security

requirements, describing security architectures, distinguishing security interoperability and comparing the security aspects of information. Once the requirements are identified, the security architecture may be developed by identifying the security mechanisms that respond to the requirements. A variety of security mechanisms may exist for each requirement. Consequently, trade-offs can be made to optimize the architecture.

Additional work is underway at the NSA and the Defense Information Systems Agency.

PHOTO : Fig. 1 The framework is a three-dimensional matrix.

PHOTO : Fig. 2 The system elements dimension of the framework.

REFERENCES

[1.] Defense-Wide Information Systems Security

Program (DISSP) Action Plan, dated

Aug. 15, 1991, DISSP Working Group. [2.] Network Systems Security Framework,

undated, Dennis Grayson, NSA. [3.] International Organization for Standardization

(ISO), Security Architecture, DIS

7498-2, 1988(E). [4.] Information Systems Security Products

and Catalog, Oct. 1991, NSA.

Carl Cecere and William H. Ruppert work within the Office of INFOSEC Systems Engineering, National Security Agency.

Go for public keys: public keys are the safest way to secure your data today. (The Critical Distinction)(computer security issues)(one of five articles in "Your Best Defense System")(Column)

Garfinkel, Simson

Windows Sources , Volume: 3 , Number: 9 , Page: 86(1) , Sep , 1995

Public-key cryptography was invented at Stanford University in 1977 and rapidly became the preferred type of encryption for most individual network users and even corporations. Each users has two keys: a private key known only only to them and a public key which is made available to all. The private key is used to encrypt a message, and the recipient uses the corresponding public key to decrypt it. Two parties can exchange information over a communications link in absolute secrecy even if others are eavesdropping. The original Diffie-Hellman public-key algorithm requires active participation on both sides of the communications link, making it less useful for encrypting E-mail or documents. RSA Data Security, formed by and named for the three inventors of its eponymous encryption algorithm, widely licenses a much better encryption scheme and offers development tools for it. Most programs that use RSA are not compatible with each other, but the freely available PGP is becoming a standard.

The Critical Distinctions

Best-Kept Secrets

Stanford researchers Whitfield Diffie and Martin Hellman invented public-key cryptography in 1977. Under this system, each user has two keys: a private key, known only to its owner, and a public key, known to all users. You use your private key to encrypt a message, and the recipient uses your public key to decrypt it. Someone who knows your public key can use it to encrypt a message he or she sends to you. Only your private key can decrypt messages encrypted with your public key.

The Diffie-Hellman system allows two parties to exchange information over a communications link with absolute secrecy, even if a third party is monitoring the link. Many communications device manufacturers--such as AT&T, with its Clipper phone, the Surety 3600s--build this algorithm into their devices. But Diffie-Hellman requires active participation (as in a phone conversation) on both sides of the communications link. For that reason, it's not useful for encrypting documents or electronic mail.

RSA All the Way

If you want to send and receive encrypted mail, then you'll probably find yourself using the RSA algorithm. RSA Data Security, the company that RSA's three inventors formed, widely licenses the algorithm (and augments it with development tools).

You first need to create a pair of cryptographic keys: a secret key and a public key. The public key encrypts messages; the secret key decrypts them. RSA keys can be any length: the longer they are, the more secure. Most serious RSA users employ keys that are at least 1,024 bits long. Experts say that messages encrypted with these keys should be safe for at least 30 years.

Although RSA Data Security has developed a set of standards for public-key cryptography, most

programs that use RSA still have incompatible keys and data file formats. As a result, you can't take your RSA key from Lotus Notes and use it with PGP, for example.

Nevertheless, because PGP is freely available for non-commercial use, its file formats are quickly becoming international standards for exchanging cryptographic keys and files. With PGP, you can create your own public key, then distribute it freely. Don't worry about your public key falling into the wrong hands: No matter who gets it, he or she won't be able to use it to decipher your incoming mail.

On the other hand, be sure you keep your private key to yourself!